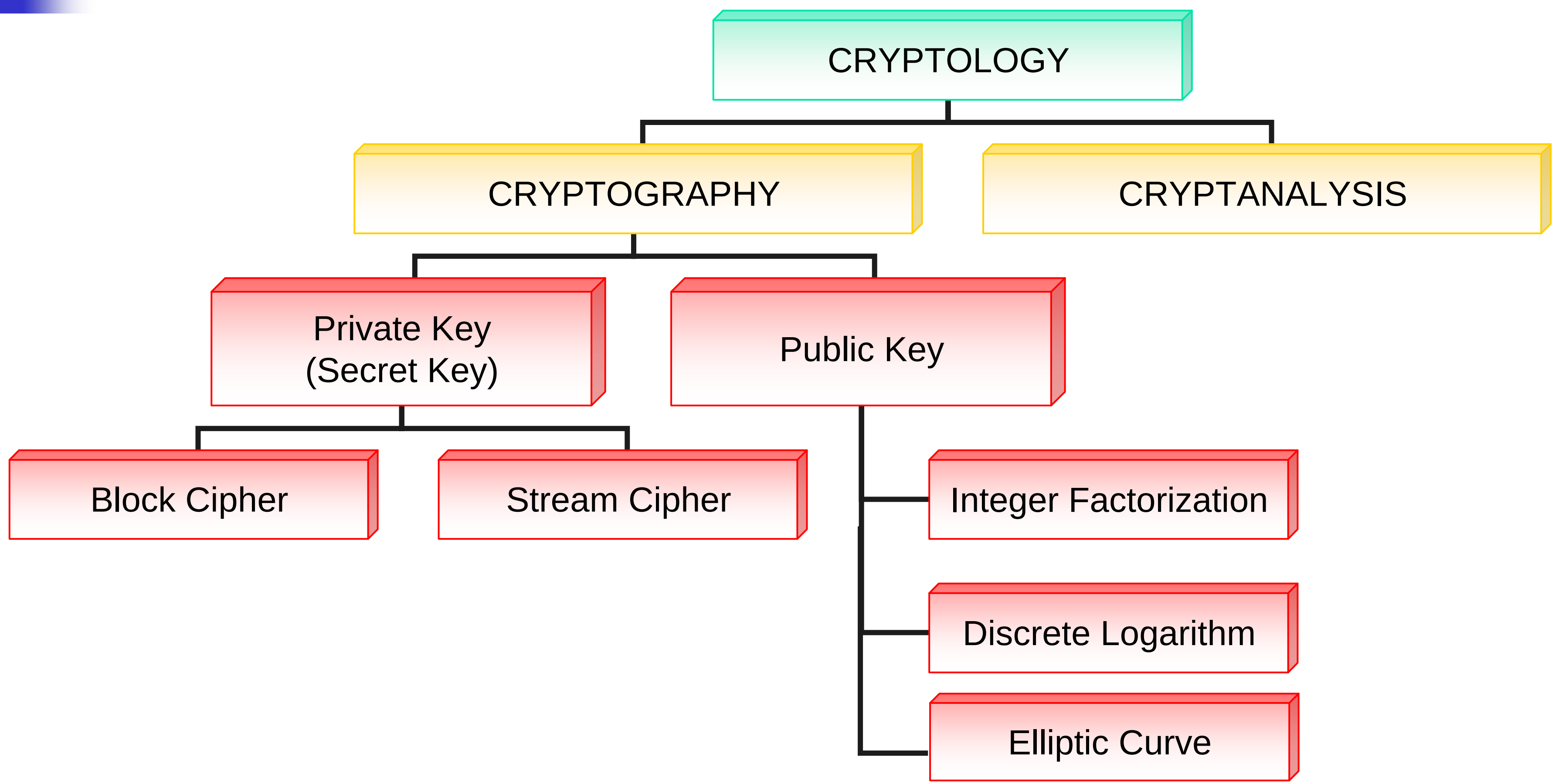
Symmetric Cryptosystem

Prof Chik How Tan
NISlab
Gjøvik University College
Chik.tan@hig.no

In this note, some of the diagrams and materials are taken from Internet

Cryptology


CRYPTOLOGY
CRYPTOGRAPHY
CRYPTANALYSIS
Private Key
(Secret Key)
Public Key
Block Cipher
Stream Cipher
Integer Factorization
Discrete Logarithm
Elliptic Curve

Data Encryption Standard (DES)

- 1972, U. S. Federal Dept. of Commerce, calling for encryption standard for storing, processing and distributing information.
- In 1974, IBM responded Lucifer cipher
- In 1976, NSA made changes of Lucifer to DES (published)
- In 1977, US National Bureau of Standard (National Institute of Standard and Technology (NIST)) adopted.

Data Encryption Standard (DES)

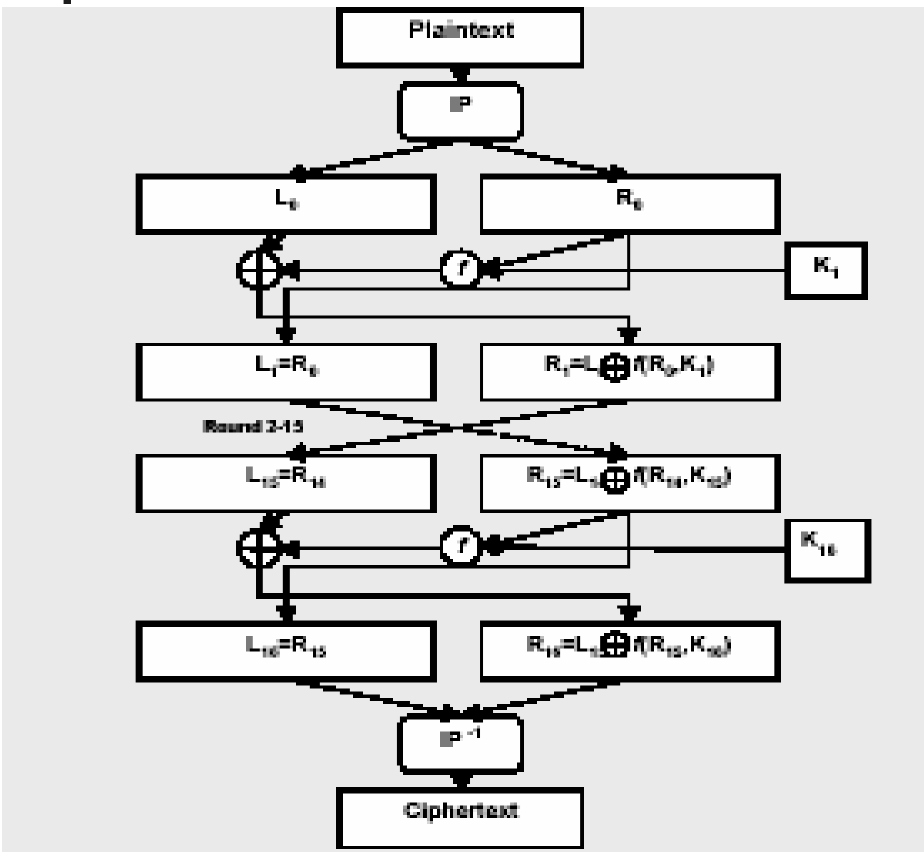
Design Requirements:

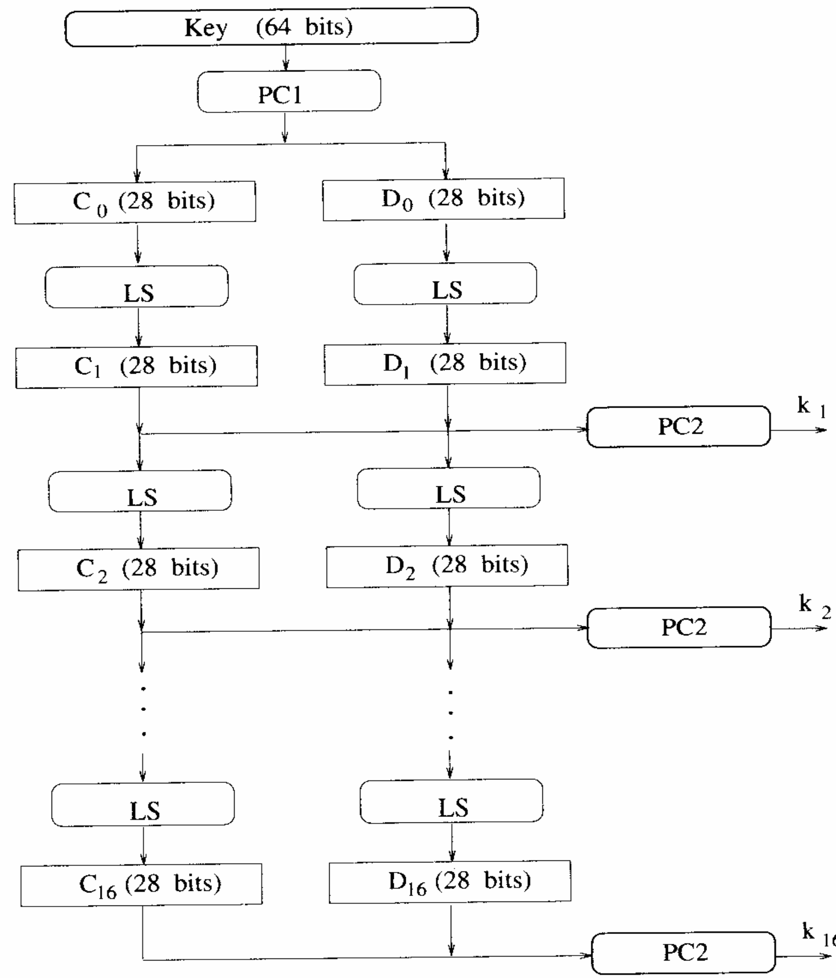
- High level of security;
- Comprehensive and transparent specification;
- Security may not rely on the secrecy of the algorithm;
- Available and accessible to all users;
- Suitable for a variety of applications;
- Low cost implementation
- Able to be exported
- Accessible for validation

DES Structure

- DES is a block cipher with 64 bits input/output and secret key 56 bits
- DES has 16 rounds
- One Key schedule algorithm: Permuted choice one and two (PC-1, PC-2), schedule of left shift
- Permutation: Initial permutation IP and its inverse IP^{-1}
- Each round function $f : \{0,1\}^{48} \times \{0,1\}^{32} \rightarrow \{0,1\}^{32}$:
  - Expansion function E
  - 8 Substitution table (S-Box)
  - Permutation function P

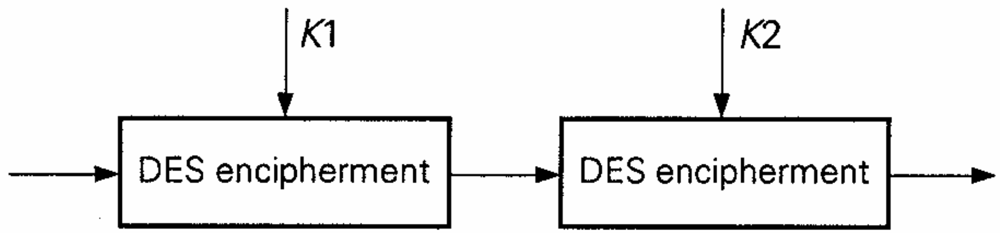
DES Block Diagram





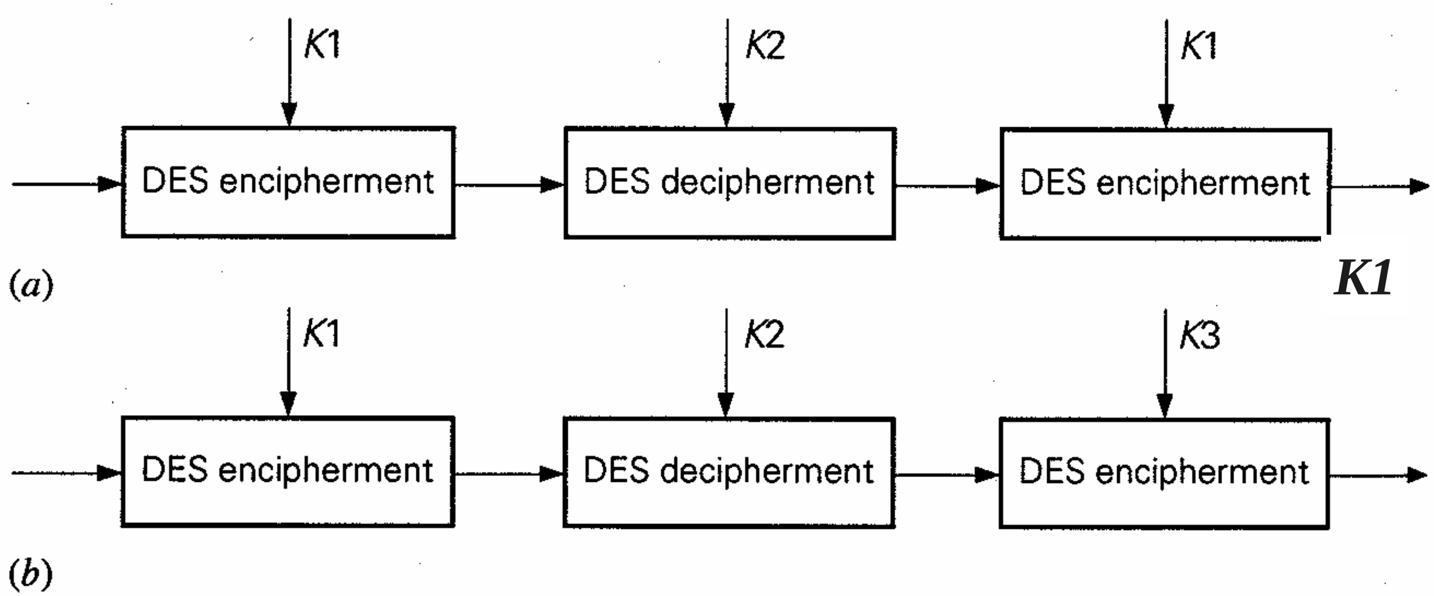
Two-DES and Triple-DES

Twofold encipherment based on the DES.



K3

(a). Threefold encipherment with the DES; (b) triple-DES.



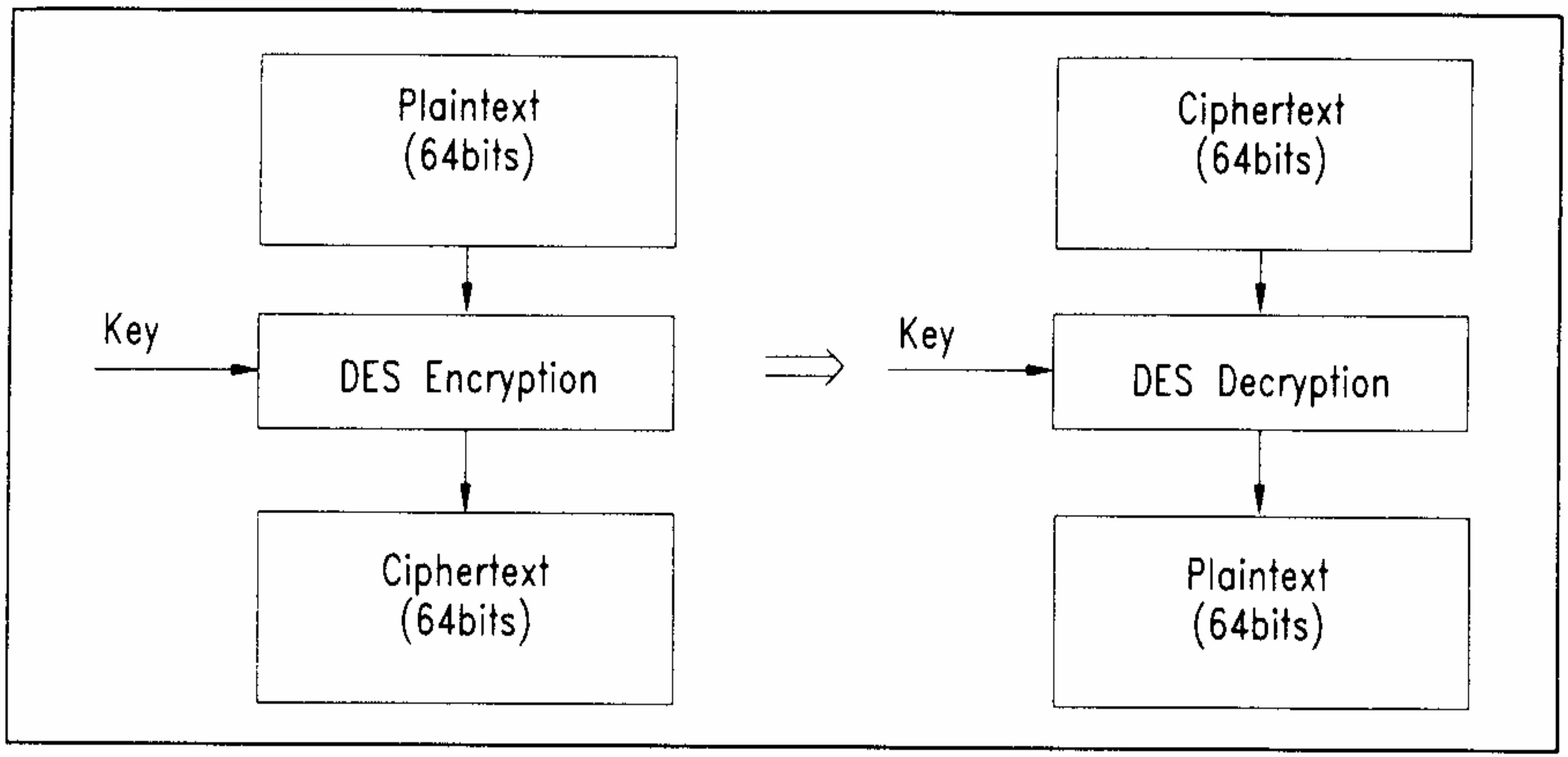
DES Security

- Weak keys: 0101010101010101, 1F1F1F1F0E0E0E0E, E0E0E0E0F1F1F1F1, FEFEFEFEFEFEFEFE + 12 other weak keys
- 1990, Biham and Shamir presented a differential cryptanalysis attack on DES (ciphertext: 2^{48})
- 1993 Matsui presented a linear cryptanalysis attack on DES (ciphertext : 2^{43})
- 1993, Wiener propose a VLSI key search engine of cost one million to find key in 3.5 hours.
- 1996(?) Distributed.Net and EFF finding key in 56 hours using 100,000 PC.
- 1998 DES Cracker (EFF) finding key in 22 hours 15 min
  - Specialized hardware: cost $250,000
  - Brute force attack: try all possible keys (2^{56})
- The rumor is that NSA can crack DES in 3-15 minutes with hardware for $50,000
- Single DES not longer secure in use, will use Triple DES (112 bits or 168 bits)

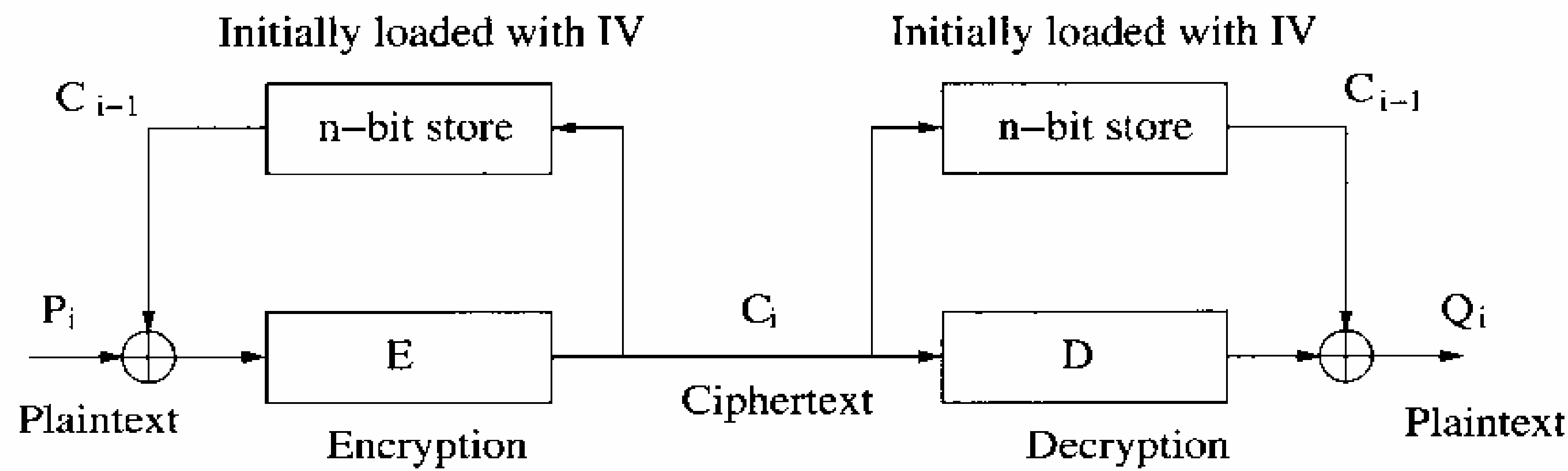
Mode of Operations

- Electronic Codebook (ECB)
- Cipher Block Chaining (CBC)
- Cipher Feedback Mode (CFB)
- Output Feedback Mode (OFB)
- Counter Mode (CTR)

Electronic Codebook (ECB)



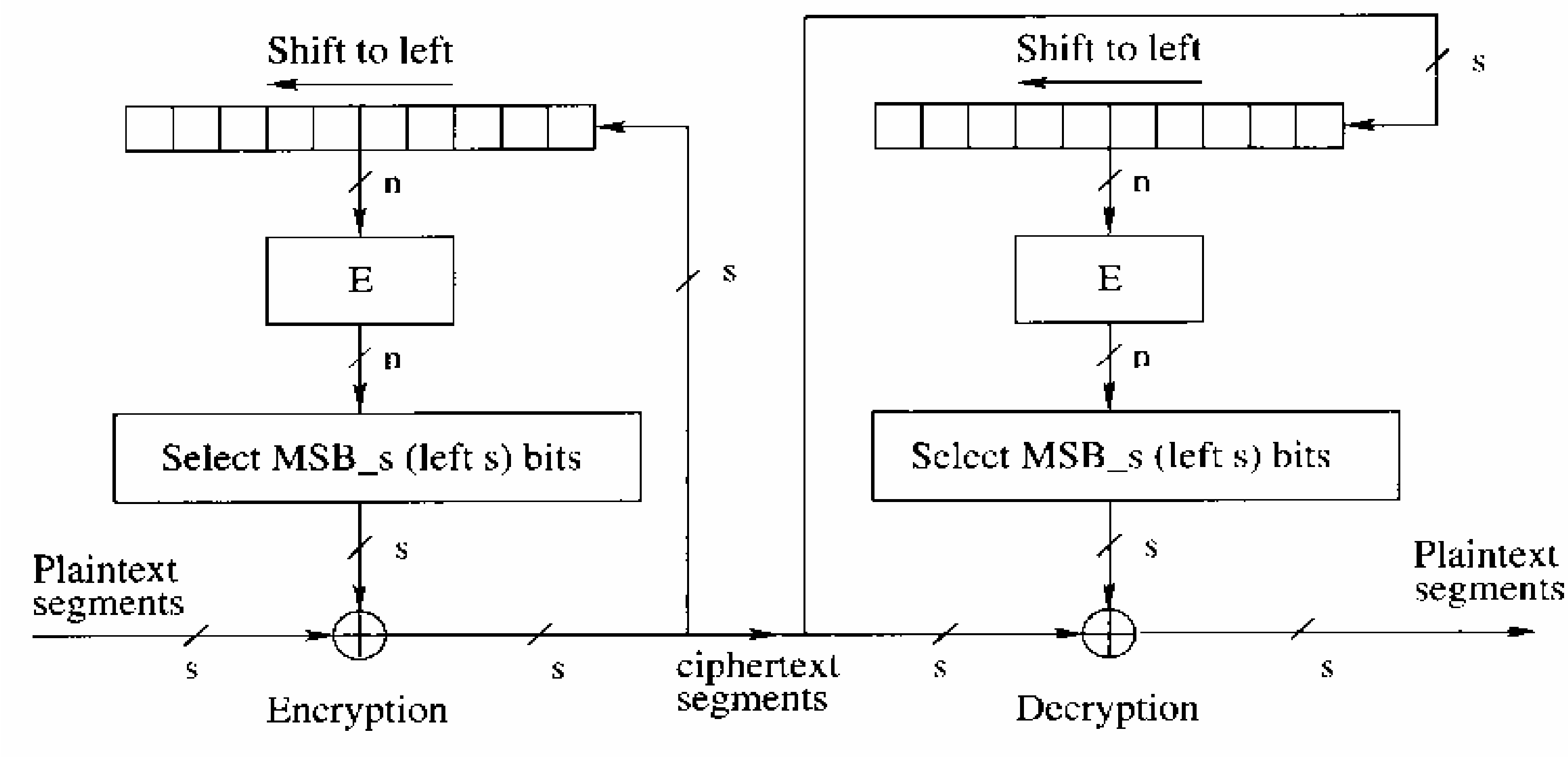
Cipher Block Chaining (CBC)



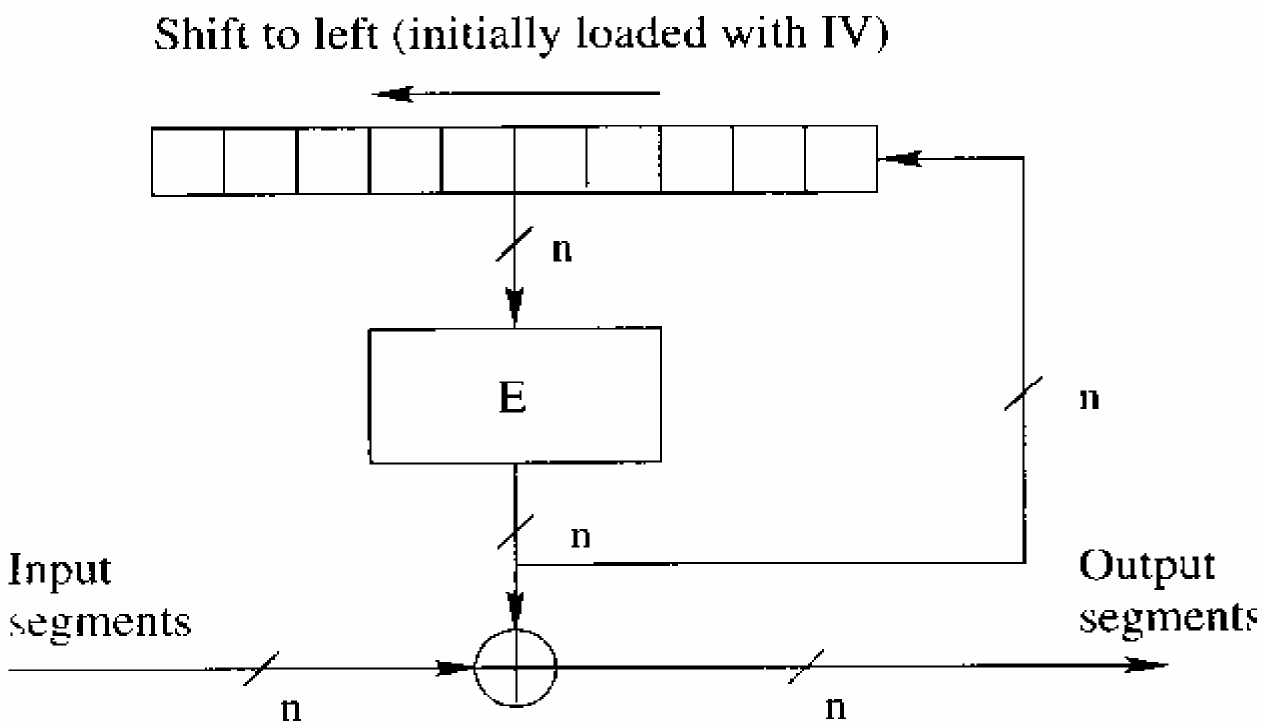
$C_0 = IV$
$P_0 = 0$

$Q_i = P_i$

Cipher Feedback (CFB)



Output Feedback (OFB)



Counter Mode (CTR)

- CTR Encryption :
  - INPUT : $Ctr_1, m_1, m_2, \ldots$
  - OUTPUT : $Ctr_1, c_1, c_2, \ldots$
  - $c_i = m_i \oplus E(Ctr_i)$, $i = 1, 2, ..$
- CTR Decryption :
  - INPUT : $Ctr_1, c_1, c_2, \ldots$
  - OUTPUT : $Ctr_1, m_1, m_2, \ldots$
  - $m_i = c_i \oplus E(Ctr_i)$, $i = 1, 2, ..$

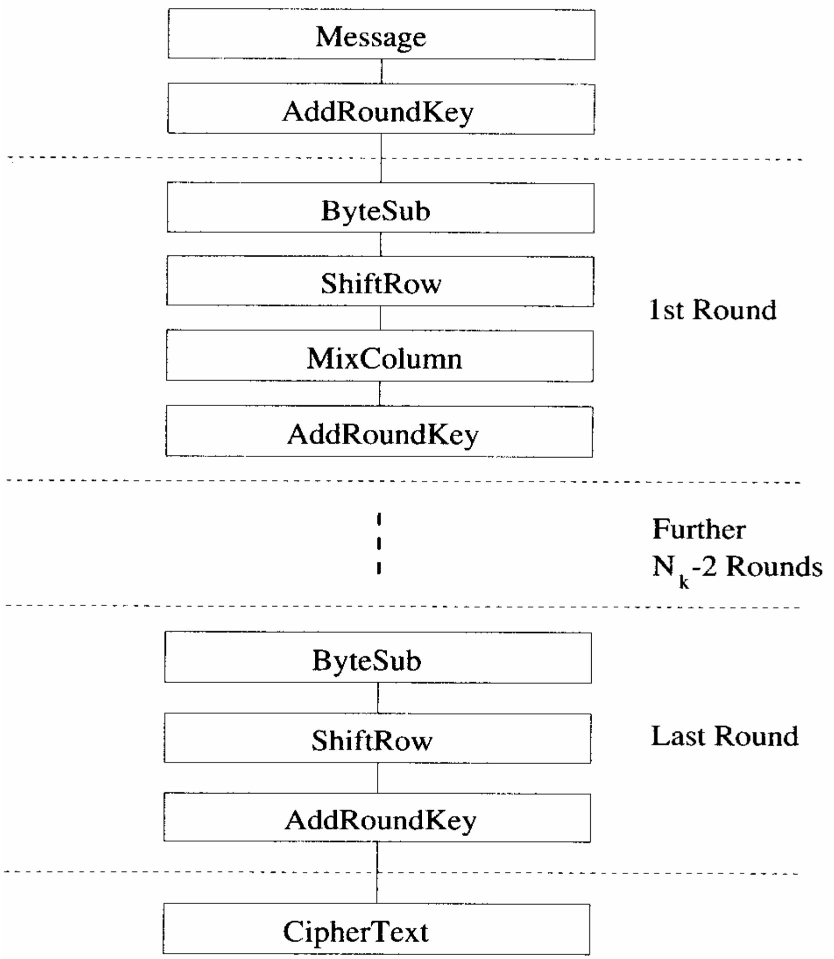
Advance Encryption Standard (AES)

- 1997-- NIST called for proposal, there are 15 algorithms submitted
- 2001 – NIST selected Rijndeal as an AES in FIPS 197
- AES has more than 10 rounds
- Input 128 bits and output 128 bits with key 128, 192 or 256 bits
- Key schedule algorithm
- Each round function f : $\{0,1\}^{128} \times \{0,1\}^{128} \rightarrow \{0,1\}^{128}$:
  - ByteSub
  - Shiftrows
  - MixColumns
  - AddRoundKey

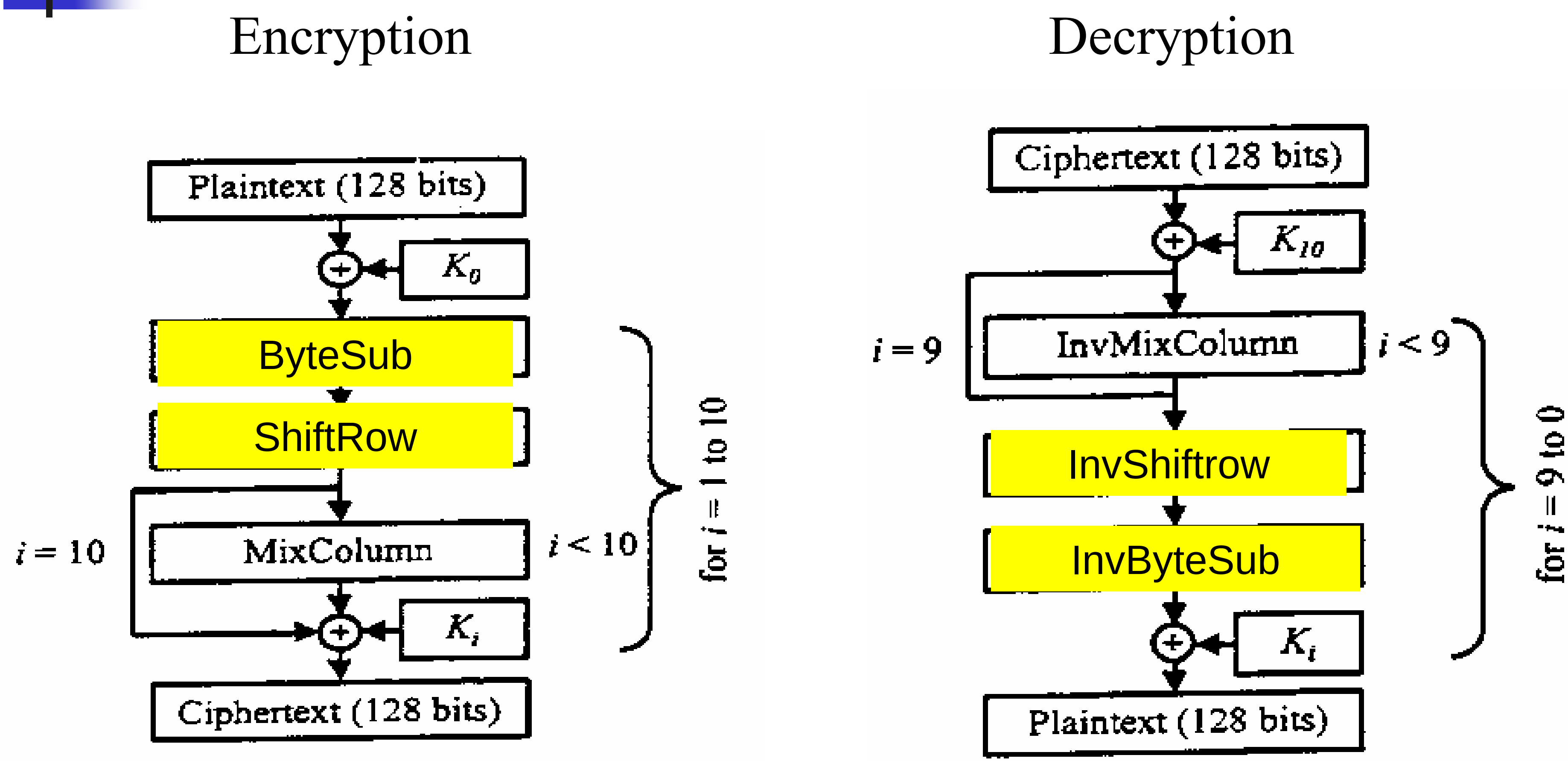
Number of rounds

	Key Length (*Nk words*)	Block Size (*Nb words*)	Number of Rounds (*Nr*)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

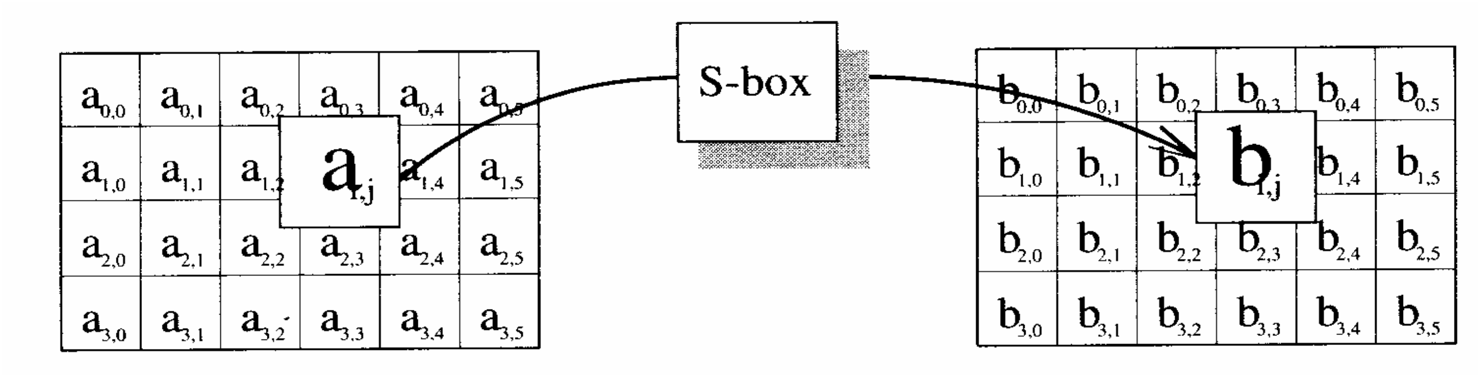
AES Structure



AES Block Diagram



ByteSub Transformation



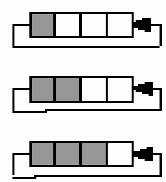
ByteSub (S-Box)

S-Box

99	124	119	123	242	107	111	197	48	1	103	43	254	215	171	118
202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
83	209	0	237	32	252	177	91	106	203	190	57	74	76	88	207
208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115
96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
224	50	58	10	73	6	36	92	194	211	172	98	145	149	228	121
231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

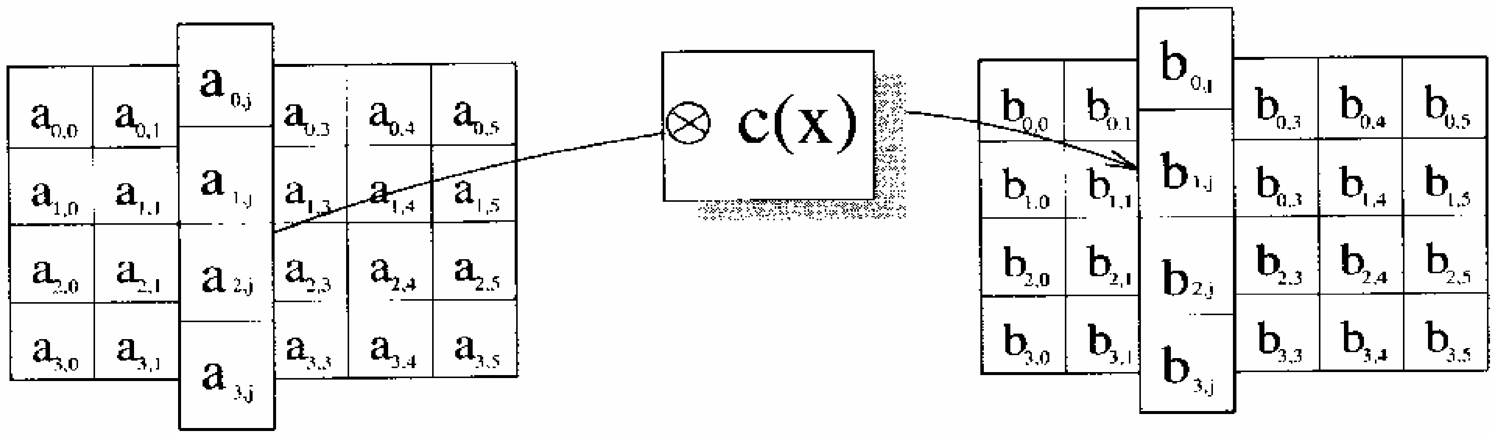
ShiftRow Transformation

$$\begin{pmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{pmatrix}.$$



$$\begin{pmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,1} & s_{1,2} & s_{1,3} & s_{1,0} \\ s_{2,2} & s_{2,3} & s_{2,0} & s_{2,1} \\ s_{3,3} & s_{3,0} & s_{3,1} & s_{3,2} \end{pmatrix}.$$

MixColumn Transformation



$$\begin{bmatrix} b_{0,j} \\ b_{1,j} \\ b_{2,j} \\ b_{3,j} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_{0,j} \\ a_{1,j} \\ a_{2,j} \\ a_{3,j} \end{bmatrix}$$

Addition

{01100011} identifies the specific finite field element $x^6 + x^5 + x + 1$.

Addition

$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = x^7 + x^6 + x^4 + x^2$ (polynomial notation);

{01010111} $\oplus$ {10000011} = {11010100} (binary notation);

{57} $\oplus$ {83} = {d4} (hexadecimal notation).

Multiplication

$$m(x) = x^8 + x^4 + x^3 + x + 1,$$

For example, $\{57\} \bullet \{83\} = \{c1\}$, because

$$\begin{aligned}
(x^6 + x^4 + x^2 + x + 1)\,(x^7 + x + 1) &= x^{13} + x^{11} + x^9 + x^8 + x^7 + \\
&\quad x^7 + x^5 + x^3 + x^2 + x + \\
&\quad x^6 + x^4 + x^2 + x + 1 \\
&= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1
\end{aligned}$$

and

$$\begin{aligned}
x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \ \texttt{modulo}\ (x^8 + x^4 + x^3 + x + 1) \\
= x^7 + x^6 + 1.
\end{aligned}$$

$$\begin{aligned}
\{57\} \bullet \{02\} &= \texttt{xtime}(\{57\}) = \{ae\} \\
\{57\} \bullet \{04\} &= \texttt{xtime}(\{ae\}) = \{47\} \\
\{57\} \bullet \{08\} &= \texttt{xtime}(\{47\}) = \{8e\} \\
\{57\} \bullet \{10\} &= \texttt{xtime}(\{8e\}) = \{07\},
\end{aligned}$$

$$\begin{aligned}
\{57\} \bullet \{13\} &= \{57\} \bullet (\{01\} \oplus \{02\} \oplus \{10\}) \\
&= \{57\} \oplus \{ae\} \oplus \{07\} \\
&= \{fe\}.
\end{aligned}$$

AddRoundKey

$$\begin{pmatrix} d_{0,0} & d_{0,1} & d_{0,2} & d_{0,3} \\ d_{1,0} & d_{1,1} & d_{1,2} & d_{1,3} \\ d_{2,0} & d_{2,1} & d_{2,2} & d_{2,3} \\ d_{3,0} & d_{3,1} & d_{3,2} & d_{3,3} \end{pmatrix} \oplus \begin{pmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3} \\ k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \end{pmatrix}$$

$$= \begin{pmatrix} e_{0,0} & e_{0,1} & e_{0,2} & e_{0,3} \\ e_{1,0} & e_{1,1} & e_{1,2} & e_{1,3} \\ e_{2,0} & e_{2,1} & e_{2,2} & e_{2,3} \\ e_{3,0} & e_{3,1} & e_{3,2} & e_{3,3} \end{pmatrix}.$$

Key Schedules

Rcon[1] = 01000000

Rcon[2] = 02000000

Rcon[3] = 04000000

Rcon[4] = 08000000

Rcon[5] = 10000000

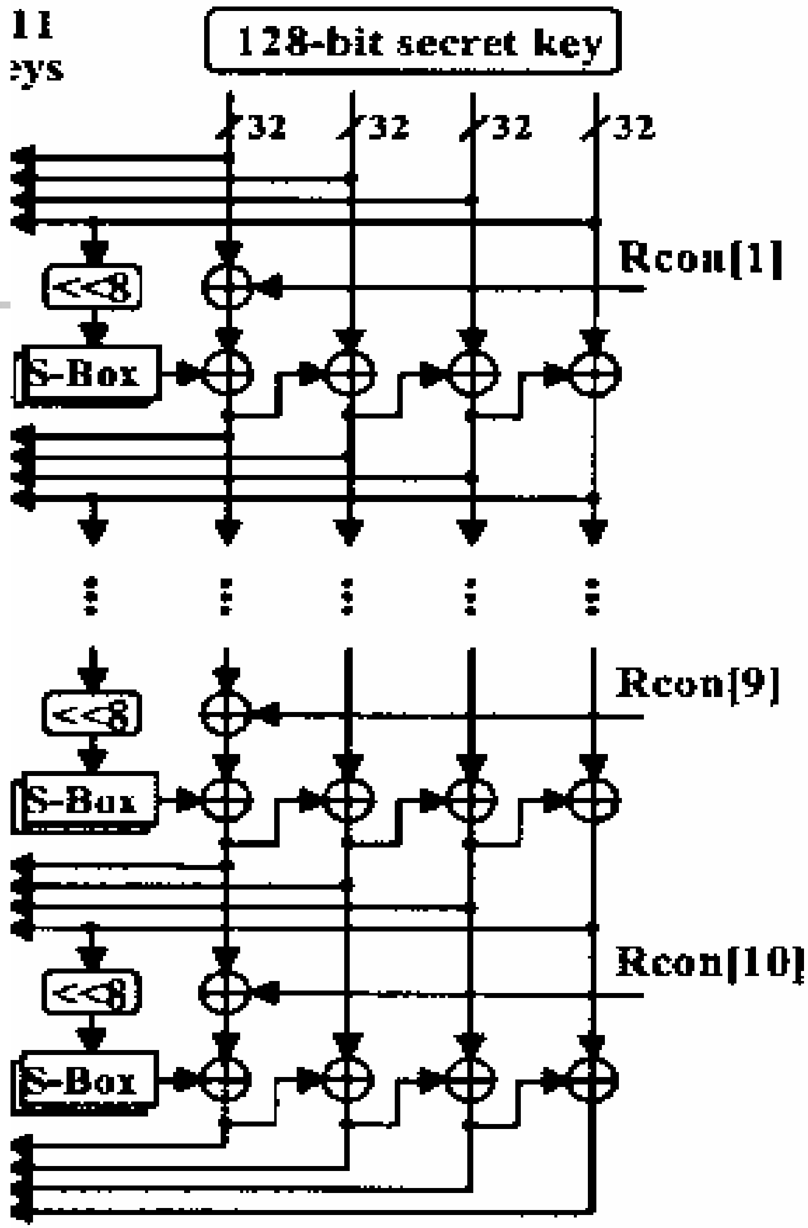
Rcon[6] = 20000000

Rcon[7] = 40000000

Rcon[8] = 80000000

Rcon[9] = 1b000000

Rcon[10] = 36000000



AES Decryption

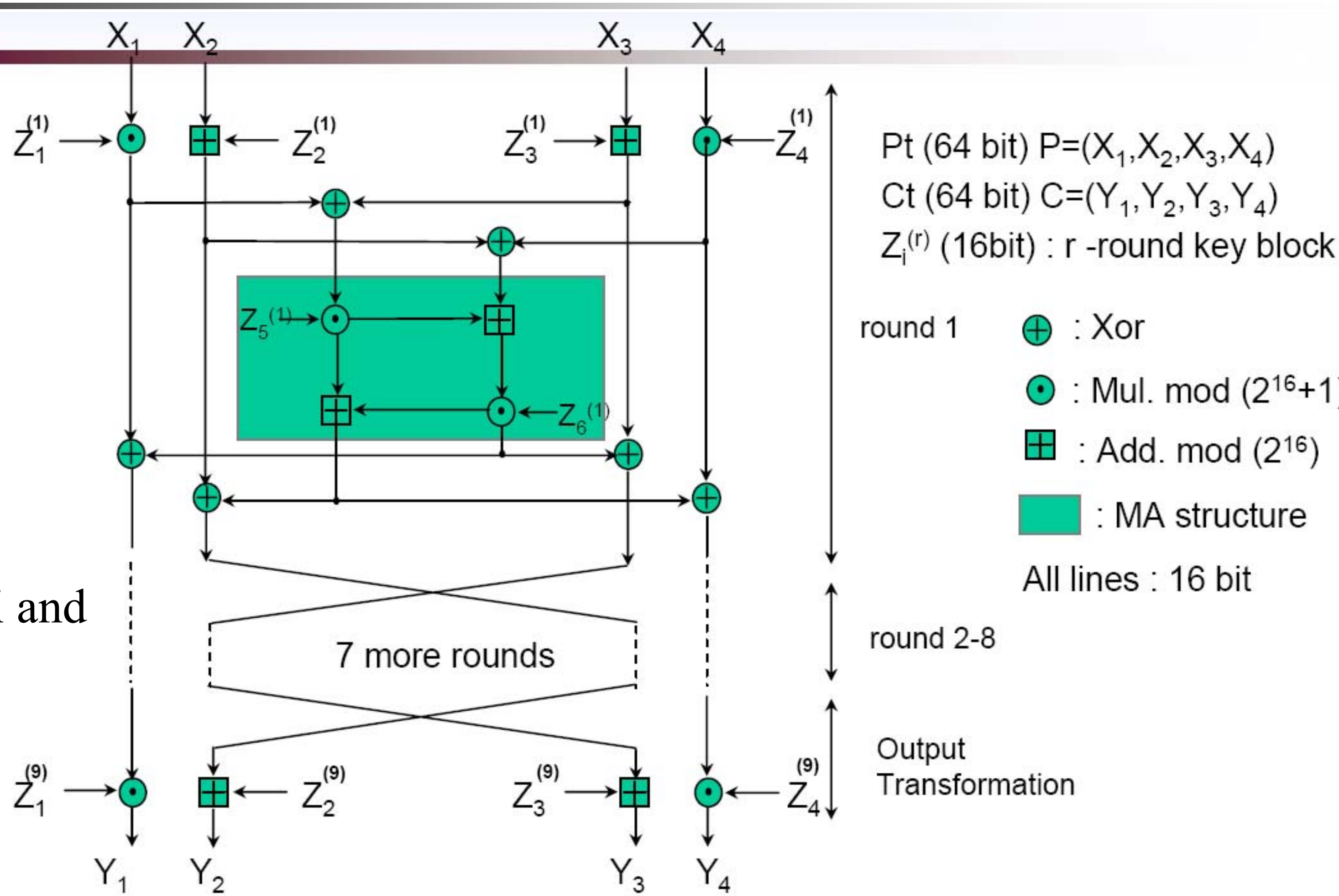
- The decryption mainly in the inverse direction
  - InvAddRoundKey
  - InvMixColumns
  - InvShiftrows
  - InvByteSub
- The decryption is different from the encryption

Performance and Security of AES

- AES runs faster than DES, and other many other block ciphers, ex, RC6, MAR, Serpent, SAFER+, CAST, DEAL, Twofish, E2, etc.
- Pentium 4 (3.2GHz) : 861 Mbps (in C), 1.537Gbps (in assembly)
- Pentium III (1.33MHz): 466 Mbps (in C), 718Mbps(in assembly)
- Alpha AXP 21164 (600MHz) : 166Mbps
- FPGA: Xilinx (Virtex E-600-8): 1.3Gbps, 17.8Gbps with pipelining
- ASIC: 3.46Gbps (in 36.9Kgates)
- AES is secure against exhaustive key search
- AES is secure against Differential/Linear Cryptanalysis

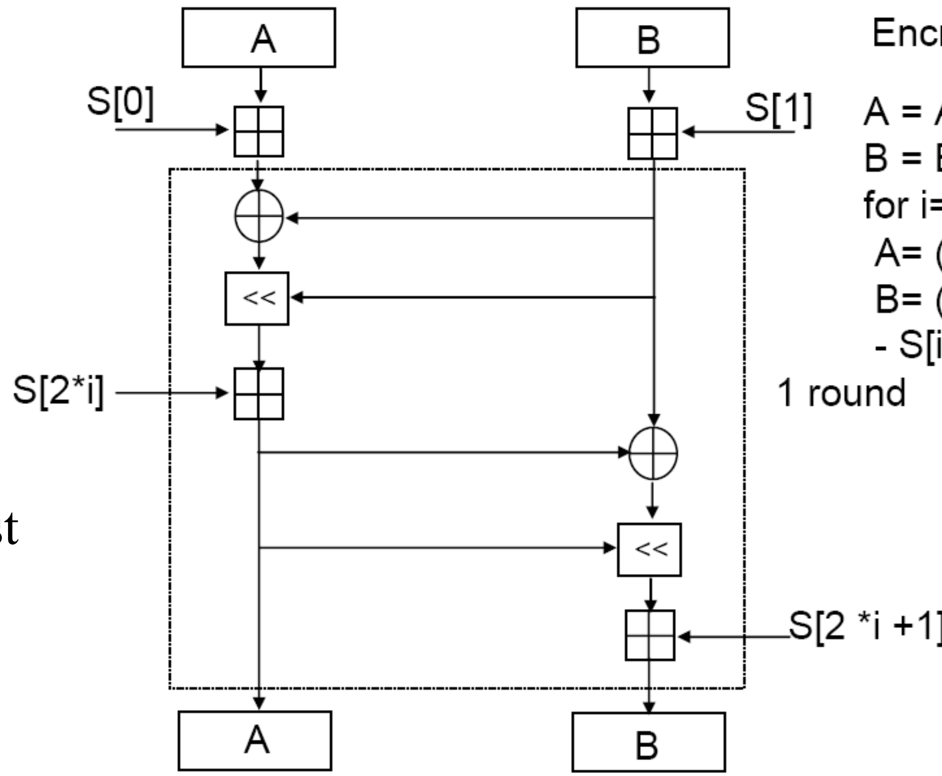
Authors	Key	Device	Slices	BRAM	Area	Throughput (Gbps)	TPS (Mbps/slice)	TPA (Mbps/area)
Chodowiec and coworkers [13, 14]	[Cho]	Virtex 1000-6	12 600	80	22 840	12.16	0.965	0.532
Chodowiec *et al.* [13]	[Cho]	Virtex 1000-6	2 057	8	3 081	1.265	0.615	0.411
Chodowiec and coworkers [13, 14]	[Cho]	Virtex 1000-6	2 507	0	2 507	0.414	0.165	0.165
Dandalis *et al.* [8]	[Dan]	Virtex -6	5 673	0	5 673	0.353	0.062	0.062
Elbirt *et al.* [6, 9]	[Elb]	Virtex 1000-4	10 992	0	10 992	1.938	0.176	0.176
Elbirt *et al.* [6, 9]	[Elb]	Virtex 1000-4	4 871	0	4 871	0.949	0.195	0.195
Gaj and Chodowiec [11]	[Gaj]	Virtex 1000-6	2 902	0	2 902	0.332	0.114	0.114
Hodjat and Verbauwhede [15]	[Hod]	Virtex-II VP20-7	9 446	0	9 446	21.64	2.291	2.291
Hodjat and Verbauwhede [15]	[Hod]	Virtex-II VP20-7	5 177	84	15 929	21.54	4.161	1.352
Järvinen *et al.* [27]	[Jär]	Virtex-II 2000-5	10 750	0	10 750	17.8	1.656	1.656
Järvinen *et al.* [27]	[Jär]	Virtex-E 1000-8	11 719	0	11 719	16.54	1.411	1.411
Labbé and Pérez [39]	[Lab]	Virtex 1000-4	2 151	4	2 663	0.394	0.183	0.148
Labbé and Pérez [39]	[Lab]	Virtex 1000-4	3 543	4	4 055	0.796	0.225	0.196
Labbé and Pérez [39]	[Lab]	Virtex 1000-4	8 767	4	9 279	1.911	0.218	0.206
McLoone and McCanny [20]	[ML1]	Virtex-E 3200-8	2 222	100	15 022	6.956	3.131	0.463
McLoone and McCanny [25]	[ML2]	Virtex-EM 812-8	2 000	244	33 232	12.02	6.010	0.362
McLoone and McCanny [21]	[ML3]	Virtex-EM 812-8	2 679	82	13 175	6.956	2.596	0.528
Pramstaller and Wolkerstrofer [30]	[Pra]	Virtex-E 1000-8	1 125	0	1 125	0.215	0.191	0.191
Rodríquez-H *et al.* [16]	[Rod]	Virtex-E 2600	5 677	80	15 917	4.121	0.726	0.259
Rouvroy *et al.* [32]	[Rou]	Virtex-II 40-6	146	3	530	0.358	2.452	0.675
Saggese *et al.* [17]	[Sag]	Virtex-E 2000-8	2 778	100	15 578	8.9	3.204	0.571
Saggese *et al.* [17]	[Sag]	Virtex-E 2000-8	446	10	1 726	1	2.242	0.579
Saggese *et al.* [17]	[Sag]	Virtex-E 2000-8	5 810	100	18 610	20.3	3.494	1.091
Saggese *et al.* [17]	[Sag]	Virtex-E 2000-8	648	10	1 928	1.82	2.809	0.944
Saqib *et al.* [22]	[Saq]	Virtex-EM 812	2 744	0	2 744	0.259	0.094	0.094
Saqib *et al.* [22]	[Saq]	Virtex-EM 812	2 136	100	14 936	2.868	1.343	0.192
Standaert *et al.* [18]	[St1]	Virtex 1000-6	2 257	0	2 257	1.563	0.693	0.693
Standaert *et al.* [18]	[St1]	Virtex-E 3200-8	2 784	100	15 584	11.776	4.230	0.756
Standaert *et al.* [18]	[St1]	Virtex-E 3200-8	542	10	1 822	1.45	2.675	0.796
Standaert *et al.* [33]	[St2]	Virtex-E 3200-8	1 769	0	1 769	2.085	1.179	1.179
Standaert *et al.* [33]	[St2]	Virtex-E 3200-8	15 112	0	15 112	18.560	1.228	1.228
Wang and Ni [40]	[Wan]	Virtex-E 1000-8	1 857	0	1 857	1.604	0.864	0.864
Weaver and Wawrzynek [23]	[Wea]	Virtex-E 600-8	770	10	2 050	1.75	2.273	0.854
Zambreno *et al.* [19]	[Zam]	Virtex-II 4000	1 254	20	3 814	4.44	3.541	1.164
Zambreno *et al.* [19]	[Zam]	Virtex-II 4000	16 938	0	16 938	23.57	1.392	1.392
Zambreno *et al.* [19]	[Zam]	Virtex-II 4000	2 206	50	8 606	10.88	4.932	1.264
Zambreno *et al.* [19]	[Zam]	Virtex-II 4000	3 766	100	16 566	22.93	6.089	1.384
Zambreno *et al.* [19]	[Zam]	Virtex-II 4000	387	10	1 667	1.41	3.643	0.846
Zhang and Parhi [29]	[Zha]	Virtex 1000-6	11 014	0	11 014	16.032	1.456	1.456
Zhang and Parhi [29]	[Zha]	Virtex 800-6	9 406	0	9 406	9.184	0.976	0.976
Zhang and Parhi [29]	[Zha]	Virtex-E 1000-8	11 022	0	11 022	21.556	1.956	1.956
Zhang and Parhi [29]	[Zha]	Virtex-EM 812-8	9 406	0	9 406	11.965	1.272	1.272

IDEA



- Designed by Lai and Messay in 1990
- 8 rounds

RC5



Encryption

$A = A \boxplus S[0]$
$B = B \boxplus S[1]$
for i=1 to r do
$A = (A \oplus B) \lll B) \boxplus S[2*i]$
$B = (B \oplus A) \lll A) \boxplus S[2*i+1]$
- S[i] : Round Key

$\oplus$: XOR

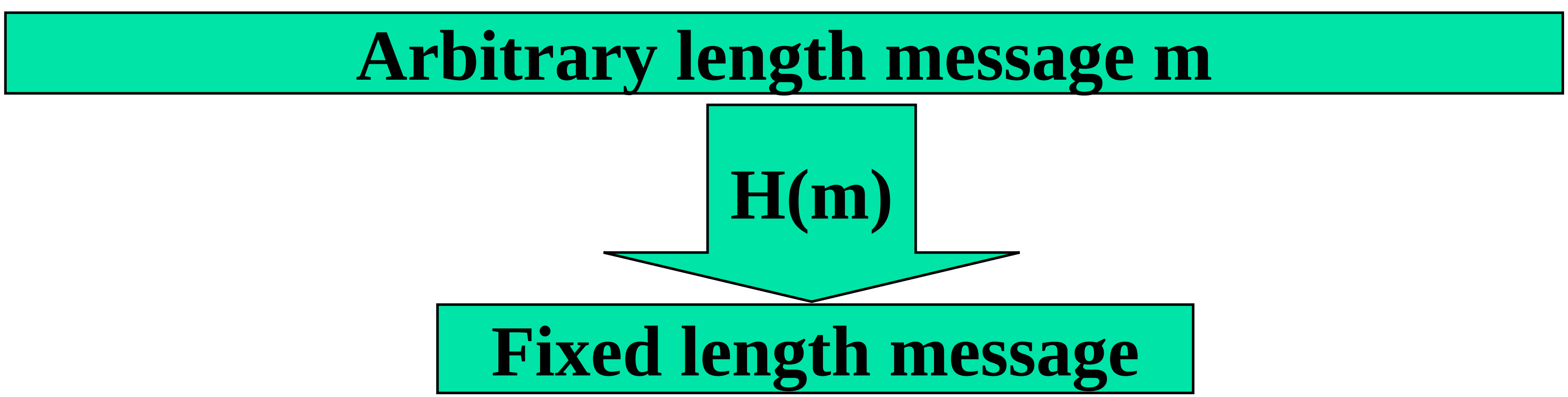
$\lll$: Rotation

$\boxplus$: addition mod 2^w

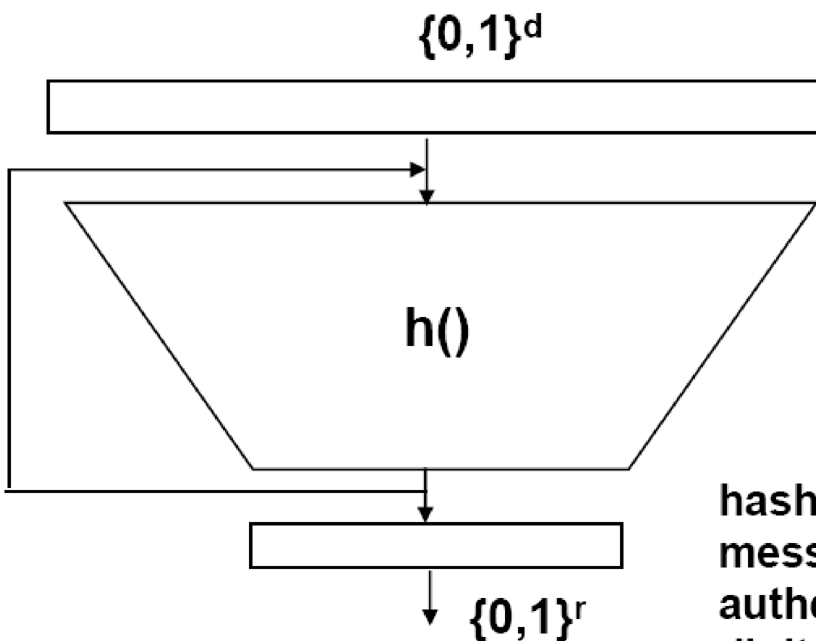
- Designed by Rivest in 1994
- 16 rounds

Hash Function

- One-way function: Given m, compute H(m) is easy. Given h=H(m), to find M is difficult
- Second Pre-image: Given m, finding m' such that H(m')=H(m) is hard
- Collision-resistance: Finding m_1 and m_2 such that $H(m_1)=H(m_2)$ is hard



Hash Function (Cont'd)



d > r

hash, hash code/value/result
message digest,checksum,MIC,
authentication tag, seal,compression
digital fingerprint, imprint

Birthday Paradox

- Given 23 people in the room, the probability of at least two persons having the same birthday is

  $p=1-(1-1/365)(1-2/365) .. (1-22/365) > 0.5$
- The probability of finding a pair of messages (about $2^{n/2}$) hash to the same digest is

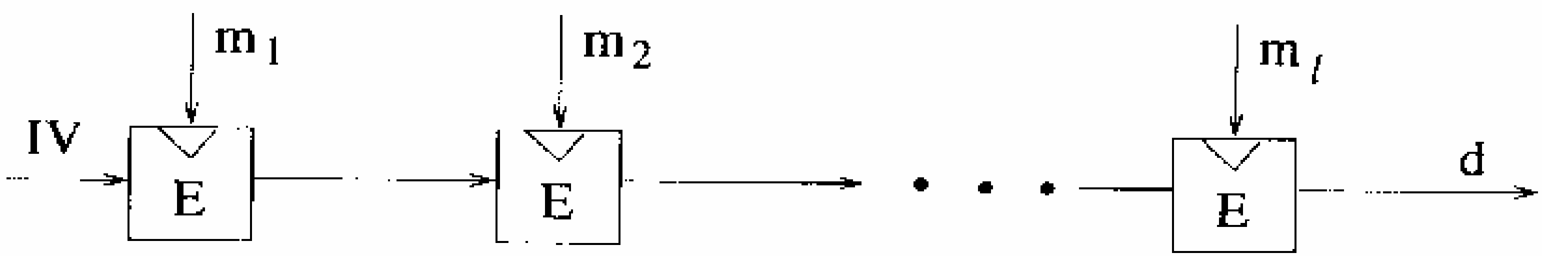
  $p = 1 – e^{-1} > 0.63.$
- When n=64 bits, $2^{n/2} = 2^{32}$ is insecure. Therefore, n is at least 128 bits

Some Hash Functions

- Hashing based on symmetric key cryptosystem
  - Rabin hashing scheme
  - Davies hashing scheme
  - Keyed hashing based on CBC mode
- Constructions
  - MD4 & MD5
  - SHA
  - HAVAL

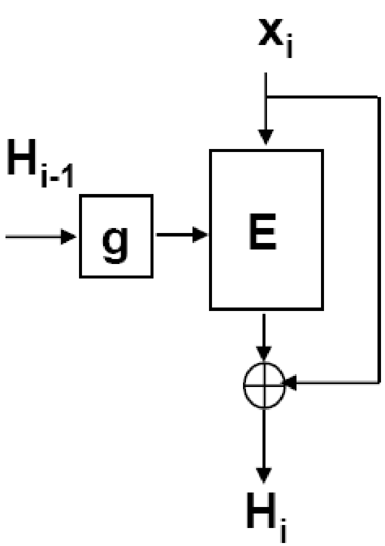
Rabin Hash Scheme

$$h_0 = IV,$$
$$h_i = E(m_i, h_{i-1}) \text{ for } i = 1, 2, \ldots, \ell,$$
$$d = h_\ell,$$



Other Hash Functions

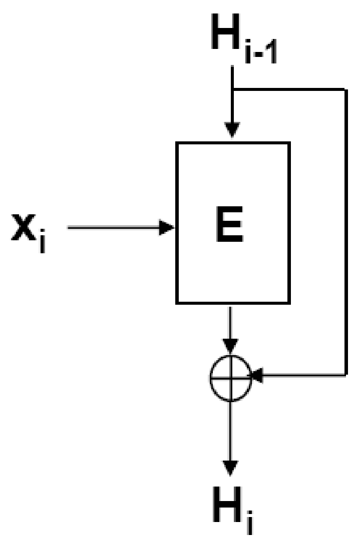
Matyas-Meyer



$H_0 = IV$

$H_i = E_{g(H_{i-1})}(x_i) \oplus x_i$

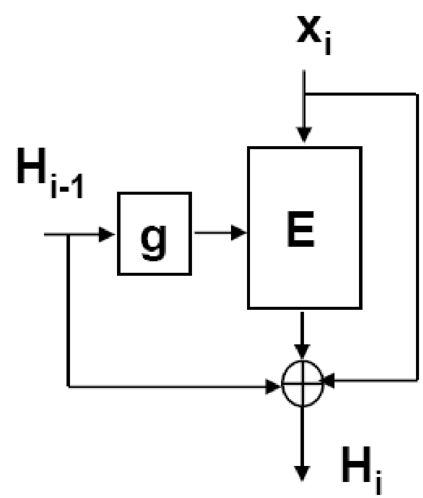
Davies-Meyer



$H_0 = IV$

$H_i = E_{x_i}(H_{i-1}) \oplus H_{i-1}$

Miyaguchi-Preneel



$H_0 = IV$

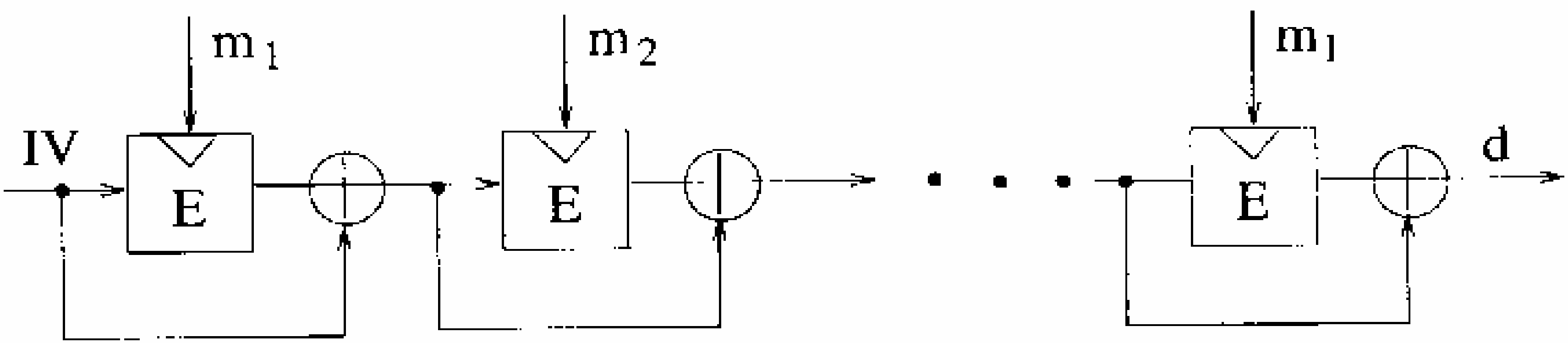
$H_i = E_{g(H_{i-1})}(x_i) \oplus x_i \oplus H_{i-1}$

Davies Hash Scheme

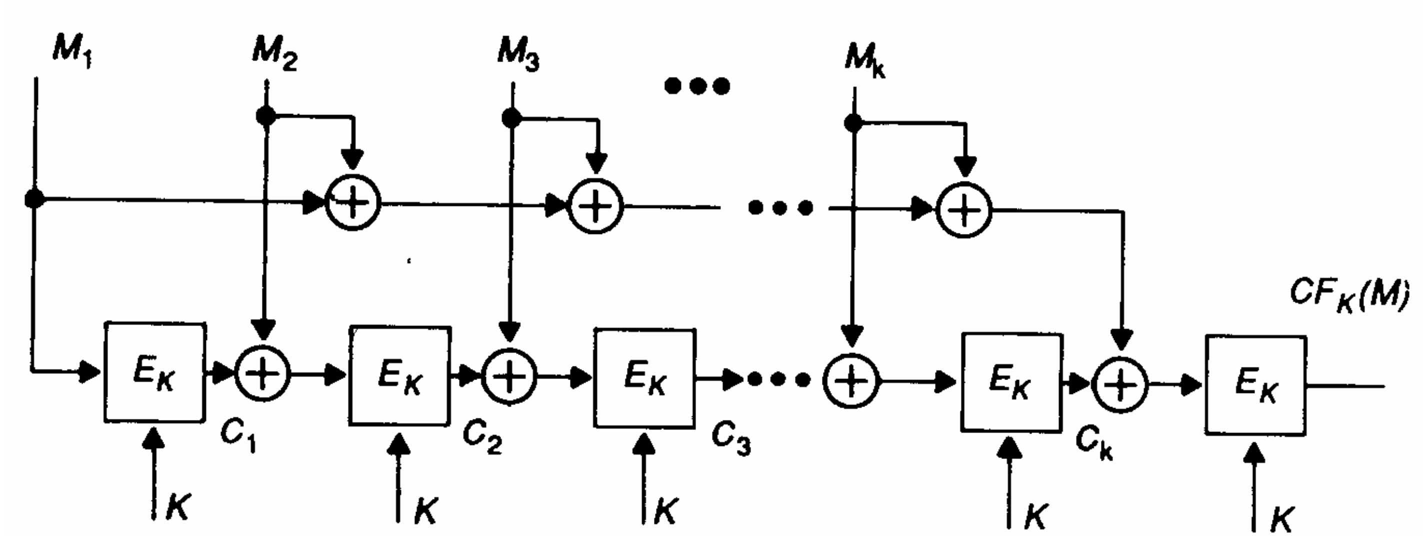
$$h_0 = IV,$$

$$h_i = E(m_i, h_{i-1}) \oplus h_{i-1} \text{ for } i = 1, 2, \ldots, \ell,$$

$$d = h_\ell.$$



Key Hashing Based on CBC Mode



$$
\begin{cases}
C_1 = E_K(M_1) \\
C_2 = E_K(M_2 \oplus C_1) \\
\quad . \\
\quad . \\
\quad . \\
C_k = E_K(M_k \oplus C_{k-1}) \\
CF_K(M) = E_K(M_1 \oplus M_2 \oplus \ldots \oplus M_k \oplus C_k)
\end{cases}
$$

SHA-1 -- Secure Hash Standard (SHS)

FIPS PUB 180

Secure Hash Standard

Federal Information Processing Standards Publications

U. S. Department of Commerce/N.I.S.T.

May 1993

SHA-1 or SHS

A, B, C, D, E –32 bits each.

m_i – 512-bit message blocks

$X \boxed{+} Y = X + Y \pmod{2^{32}}$

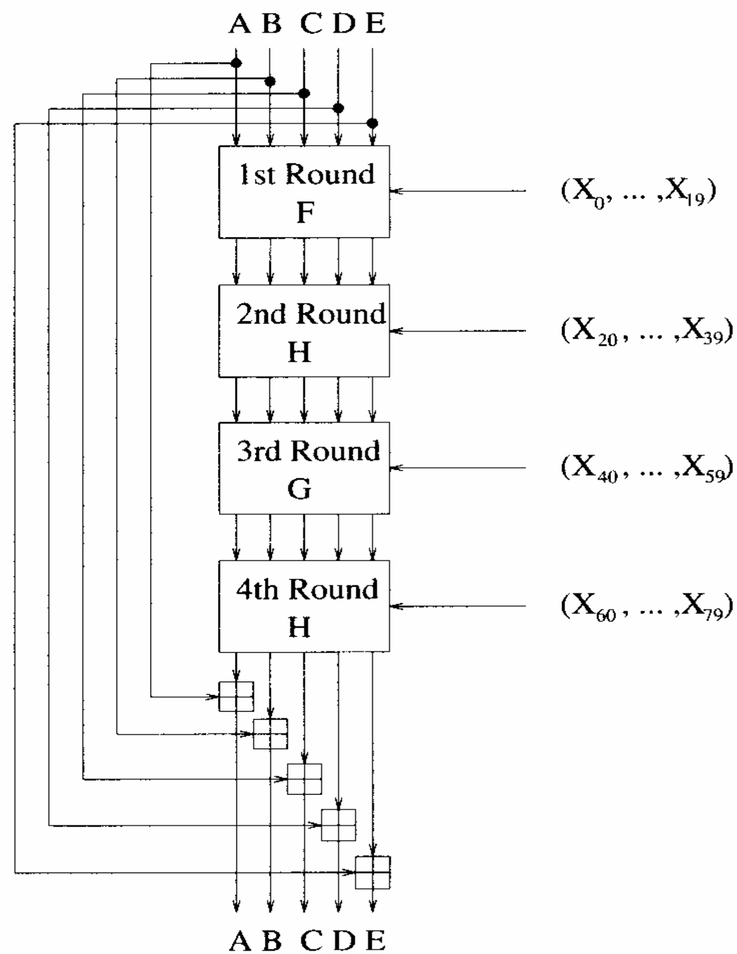
$A = 0x67452301$

$B = 0xefcdab89$

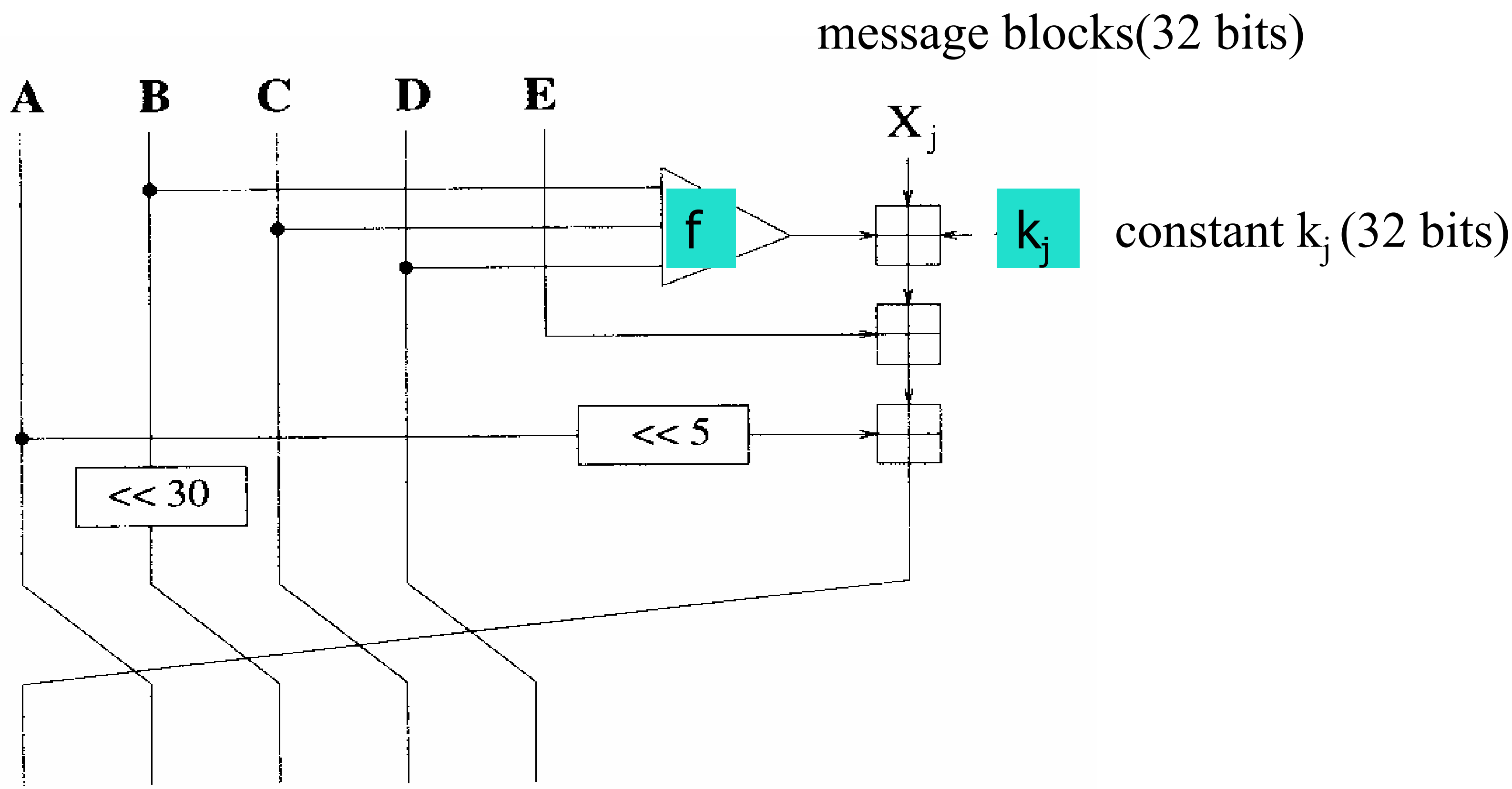
$C = 0x98badcfe$

$D = 0x10325476$

$E = 0xc3d2e1f0$



SHA-1 or SHS (Con't)



Non-Linear Functions and k_t

$$f_t(X,Y,Z) = (X \wedge Y) \vee ((\neg X) \wedge Z), \text{ for } t = 0 \text{ to } 19.$$

$$f_t(X,Y,Z) = X \oplus Y \oplus Z, \text{ for } t = 20 \text{ to } 39.$$

$$f_t(X,Y,Z) = (X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z), \text{ for } t = 40 \text{ to } 59.$$

$$f_t(X,Y,Z) = X \oplus Y \oplus Z, \text{ for } t = 60 \text{ to } 79.$$

$$K_t = \text{0x5a827999}, \text{ for } t = 0 \text{ to } 19.$$

$$K_t = \text{0x6ed9eba1}, \text{ for } t = 20 \text{ to } 39.$$

$$K_t = \text{0x8f1bbcdc}, \text{ for } t = 40 \text{ to } 59.$$

$$K_t = \text{0xca62c1d6}, \text{ for } t = 60 \text{ to } 79.$$

Hashing

For t=0 to 79

$TEMP = e + f_t(b,c,d) + (a <<< 5) + W_t + K_t \pmod{2^{32}}$

e=d

d=c

c=b <<<30

b=a

a=TEMP

a=a+ 67452301

b=b+EFCDAB89

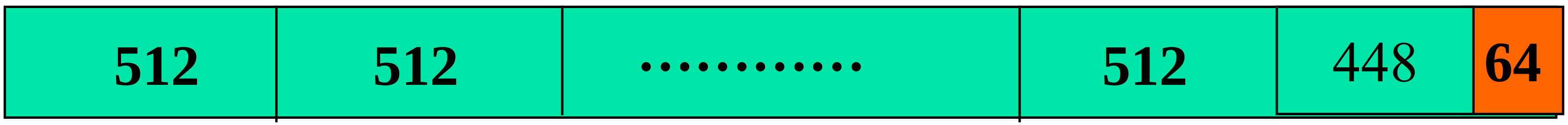
c=c+98BADCFE

d=d+10325476

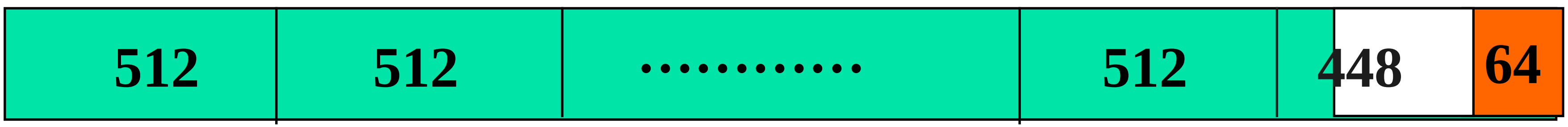
e=e+C3D2E1F0

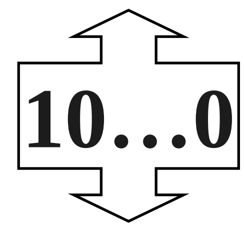
Append Padding Bits and Append Length

1. m→l(m)=448 (mod 512)

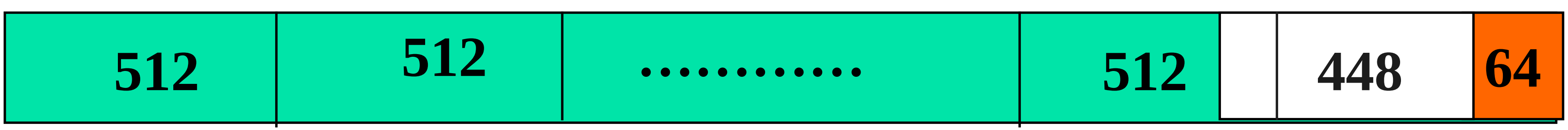


2. l(m) mod 512 < 448





3. l(m) mod 512 ≥ 448



Expanding

512	512	…………	512	512

m_0	m_1	m_2	m_3	m_4		m_{11}	m_{12}	m_{13}	m_{14}	m_{15}
32	32	32	32	32	…………	32	32	32	32	32

$$\{m_0, m_1, \ldots, m_{15}\} \rightarrow \text{expanding} \rightarrow \{w_0, w_1, \ldots, w_{79}\}$$

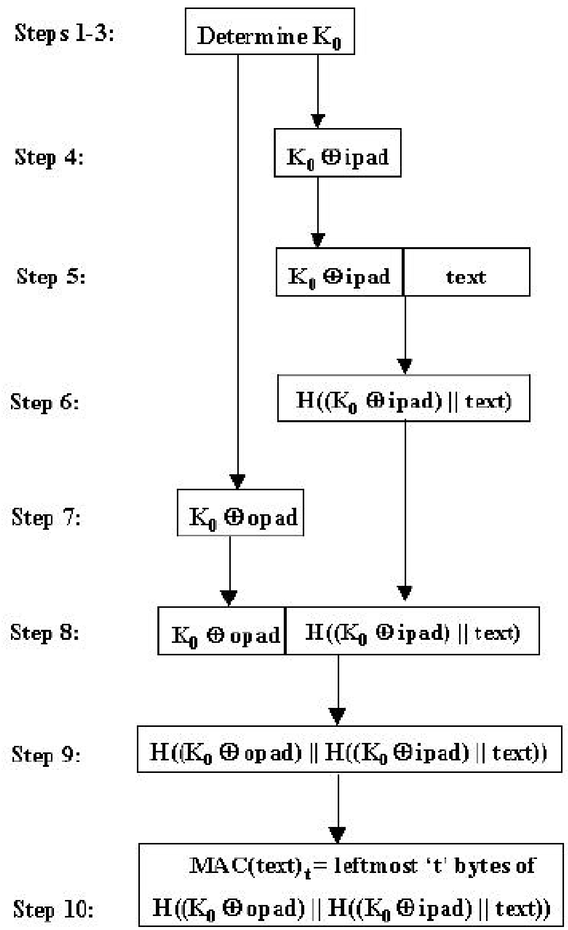
$$\begin{cases} w_i = m_i & \text{for } i=0 \text{ to } 15 \\ w_i = (w_{i-3} \oplus w_{i-8} \oplus w_{i-14} \oplus w_{i-16}) <<< 1 & \text{for } i=16 \text{ to } 79 \end{cases}$$

SHA-*

- SHA-256, SHA-384, SHA-512 are standardised by NIST in 2002, document FIP 180-2
- SHA-224 was proposed in 2004

Algorithm	Message Size (bits)	Block Size (bits)	Word Size (bits)	Message Digest Size (bits)	Security[2] (bits)
SHA-1	$< 2^{64}$	512	32	160	80
SHA-256	$< 2^{64}$	512	32	256	128
SHA-384	$< 2^{128}$	1024	64	384	192
SHA-512	$< 2^{128}$	1024	64	512	256
SHA-224	$< 2^{64}$	512	32	224	112

HMAC – FIPS 198



K_0 : the secret key

ipad : x36 36 … 36

opad : x5c 5c … 5c

H : hash function

Authors	Device	Algorithm	Slices	BlockRAMs	Throughput (Mbps)
Deepakumara *et al.* [57]	Virtex 1000-6	MD5	880	2	165
Deepakumara *et al.* [57]	Virtex 1000-6	MD5	4763	0	354
Diez *et al.* [58]	Virtex-II 3000	MD5	1369	0	467.3
Diez *et al.* [58]	Virtex-II 3000	SHA-1	1550	0	899.8
Dominikus [59]	Virtex-E 300	MD5	1004	0	146
Dominikus [59]	Virtex-E 300	RIPEMD	1004	0	89
Dominikus [59]	Virtex-E 300	SHA-1	1004	0	119
Dominikus [59]	Virtex-E 300	SHA-256	1004	0	77
Grembowski *et al.* [60]	Virtex 1000-6	SHA-1	1475[a]	0[a]	462
Grembowski *et al.* [60]	Virtex 1000-6	SHA-512	2826[a]	2[a]	616
Järvinen *et al.* [56]	Virtex-II 4000-6	MD5	1325	0	607
Järvinen *et al.* [56]	Virtex-II 4000-6	MD5	5732	0	2395
Järvinen *et al.* [56]	Virtex-II 4000-6	MD5	11498	10	5857
Järvinen *et al.* [61]	Virtex-II 2000-6	MD5	1882	0	602
Järvinen *et al.* [61]	Virtex-II 2000-6	SHA-1	1882	0	485
Kang *et al.* [62]	Apex 20K 1000-3	MD5	10573 (LE)	0	142
Kang *et al.* [62]	Apex 20K 1000-3	SHA-1	10573 (LE)	0	114
Kang *et al.* [62]	Apex 20K 1000-3	HAS-160	10573 (LE)	0	160
Lien *et al.* [54]	Virtex 1000-6	SHA-1	480	0	544
Lien *et al.* [54]	Virtex 1000-6	SHA-1	1480	0	1024
Lien *et al.* [54]	Virtex 1000-6	SHA-512	2384	0	717
Lien *et al.* [54]	Virtex 1000-6	SHA-512	3521	0	929
McLoone and McCanny [63]	Virtex-E 600-8	SHA-384/512	2914	2	479
Ng *et al.* [64]	Flex 50-1	MD5	1964 (LE)	0	206
Ng *et al.* [64]	Flex 50-1	RIPEMD	1964 (LE)	0	84
Selimis *et al.* [65]	Virtex 150	SHA-1	518	0	518
Sklavos *et al.* [66]	Virtex-II 500	SHA-1	2245	0	1339
Sklavos *et al.* [66]	Virtex-II 500	RIPEMD	2245	0	1656
Ting *et al.* [67]	Virtex-E 300-8	SHA-256	1261	0	693
Wang *et al.* [68]	Apex 20K 1000-3	MD5	3040 (LE)	1 (ESB)	178.6
Wang *et al.* [68]	Apex 20K 1000-3	SHA-1	3040 (LE)	1 (ESB)	143.3
Zibin and Ning [69]	Acex 100-1	SHA-1	1622 (LE)	0	268.99